System and Method for Using a Unique Identifier for Encryption Key Derivation

ABSTRACT

A system and method for using a unique identifier for encryption key derivation is presented. An application sends a password and a request for an encryption key to a hardware security module (HSM). The HSM uses the password to generate a tied application data encryption key (ADEK). The tied ADEK includes an encryption key and a known value that is "tied" to the password. The HSM encrypts the tied ADEK with a hardware master key and sends it to the application. When the application requests to encrypt or decrypt data, the application sends the encrypted tied ADEK and a password to the HSM. The password corresponds to the password used to generate the tied ADEK. The HSM uses an identical hardware master key and the password to recover the ADEK. The HSM also verifies that the known value is correct.